

دليل الأمن الرقمي القانوني

دليل الأمن الرقمي القانوني

2013



مؤسسة حرية الفكر والتعبير
4 شارع احمد باشا - الدور السادس - جاردن سيتي - القاهرة
تليفون/فاكس:27926281 (202)
البريد الإلكتروني: Info@afteegypt.org
الموقع الإلكتروني: www.afteegypt.org

فريق العمل

قام أحمد عزت مدير الوحدة القانونية بإعداد وتحرير الجانب القانوني، فيما قام محمد الطاهر منسق برنامج الحريات الرقمية بالمؤسسة بإعداد وتحرير الجانب التقني.

تم إخراج هذه الورقة بالاعتماد برمجيات حرة، حزمة LibreOffice، وبرنامج Gimp، متصفح FireFox، نظام التشغيل Ubuntu

تقديم

إذا كنت ناشطا أو أحد المدافعين عن حقوق الإنسان؛ فأنت بالطبع تهتم بسرية الاتصالات والمعلومات الموجودة على هاتفك المحمول، أو جهاز الحسوب الخاص بك، أو أى من الأجهزة التي تستخدمها في حفظ البيانات أو المعلومات نظرا لما قد يشكله عدم تأمين تلك المعلومات من خطورة عليك، أو على الآخرين، خاصة إذا كنت تعيش في دول قمعية تعتبر الإنترنت ووسائل الاتصالات مصدر إزعاج للسلطة، ووسيلة لفضح انتهاكات حقوق الإنسان يجب حصارها على أمنها واستمرارها.

مع بداية ثورات الربيع العربي ازدادت أهمية الأمن الرقمي، حيث تم استخدام الإنترنت والهاتف المحمول والتطبيقات المختلفة في دعاوى الحشد والتأييد والتنظيم ونقل الأخبار وغير ذلك، مما جعل الحكومات أكثر قلقا تجاه هذه الأدوات. وهو ما انعكس بالملاحقة القانونية لبعض مستخدمي مواقع التواصل الاجتماعي اللذين تعرضوا للاتهام بازدراء الأديان وإهانة الهيئات النظامية، والسب والقذف وغيرها من الاتهامات الأخرى بسبب محتوى قام أحدهم بنشره أو تداوله عبر الإنترنت أو وسائل الاتصال الأخرى.

إضافة إلى ما تقدم، فإن هناك عدد ليس بقليل من الإصدارات التي خرجت عن نشطاء ومنظمات، تتناول شرح تقني حول الحماية والأمان الرقمي. وما يقدمه هذا الدليل هو محاولة لتوضيح بعض المفاهيم النظرية. وقد قمنا بتضمين بعض البرمجيات التي تساعد المستخدمين على حماية بيناتهم أثناء الاستخدام، وكذلك إلقاء الضوء على بعض الجوانب القانونية المتعلقة بإجراءات التحقيق والمحاكمة في قضايا النشر الرقمي، وذلك كي يستعين به المحامين أثناء قيامهم بمهام الدفاع عن ضحايا انتهاك الحريات الرقمية.

المفهوم

المتعاطون مع التكنولوجيا بشكل يومي يستخدمون في الغالب أكثر من جهاز، بشكل أساسي هناك الحاسوب الشخصي والهاتف الجوال، وربما تمتلك أكثر من هاتف وأكثر من حاسوب، هذا بالإضافة للأجهزة اللوحية وآلات التصوير الرقمية، وبعض الأجهزة الأخرى كأجهزة تحديد المواقع أو بطاقات الذاكرة وغيرها، كل هذه الأجهزة مخزن عليها معلومات وبيانات وحتى سجل استخدامك لها، ومفهوم الأمن الرقمي هنا هو كيفية الحفاظ على سرية هذه المعلومات وتشفيرها وحتى عند محوها أن يتم بصورة كاملة دون وجود آثار لما قمت بمحوه. ويدخل في هذا النطاق استخدام مواقع التواصل الاجتماعي التي من خلالها يستطيع الأفراد نشر بعض المحتويات سواء كانت صور أو مقاطع صوتية أو مقاطع مصورة أو غيرها، ويتطلب الاشتراك في مثل هذه المواقع الإفصاح عن بعض البيانات الشخصية التي تحدد هوية المستخدم، وعدم تأمين هذا النوع من البيانات قد يؤدي إلى اختراق حسابات المستخدمين أو استخدام هذه البيانات في الإضرار بهم. خاصة في ظل النظام القانوني المصري الذي يؤثم أنواع معينة من المحتويات إذا تم نشرها بحيث أصبحت متاحة لأي شخص لكي يطلع عليها ويتصفحها.

الأمن الرقمي.. برمجيات وعادات

الأمن الرقمي يتأثر دائما بعاداتك في الاستخدام والبرمجيات التي تسخدمها، على سبيل المثال إن كنت تستخدم مايكروسوفت ويندوز فأنت في خطر أكثر من مستخدمي توزيعات جنو/لينكس، وقياسا على أنظمة التشغيل فإن أى برمجية تستخدمها تؤثر سلبا أو إيجابا على مقدار الحماية الرقمية التي تتمتع بها، ولاحقا سنتطرق لجزئية البرمجيات. لكن يجب أن نضع في الاعتبار أن الأمن الرقمي ممارسات مستمرة وليست مجرد خطوات تقوم بها مرة واحدة ثم تتجاهلها.

أما عادات الاستخدام فيجب أن تكون حذرا تجاهها، ويجب تقييمها دائما للوصول لأقصى درجة من الحماية والأمان خاصة إذا كنت ناشطا أو مدافعا حقوقيا، وهناك بعض التصرفات العامة التي يجب ان تضعها في الاعتبار لكننا سنركز على أربعة أشياء بشكل أساسي:

مكان الاستخدام

إذا كنت تمتلك حاسوب في مكان عملك فكن حذرا أن تضع عليه بيانات أو معلومات هامة، فغالبا ما يكون سهل الوصول للمعلومات المخزنة عليه؛ خاصة إذا كنت لا تتوجد طوال يومك بالقرب منه، وهو ذاته ما يجب عليك فعله إذا كنت تستخدم الحاسوب من مقاهي الإنترنت. **كن حذرا** أيضا منها ربما تحتوى الأجهزة على برمجيات خبيثة أو يتم مراقبتها من قبل القائمين على إدارة مثل هذه الأماكن.

وبوجه عام يجب أن تكون حذرا من الأماكن التي تحتوي على أجهزة يستخدمها أكثر من شخص.

تخزين البيانات والمعلومات ذات الحساسية

في حالة أنك تستخدم جهاز حاسوب يستخدمة أكثر من شخص، لا تحاول أن تضع به أى بيانات أو معلومات يمكنها أن تشكل خطورة على أمنك الرقمي، وحاول دائما أن تبقيها بعيدا، يمكنك أن تقوم بتخزينها على وحدات خارجية كبطاقة ذاكرة مثلا، وتقوم بتشفير البيانات التي تحتويها، أيضا لا تترك أى كلمة مرور أو اسم مستخدم على حاسوب يستخدمه أكثر من شخص، بل حاول أن استخدم برامج تصفح آمنة، وقم بمسح دوري لجميع البيانات المخزنة بالمتصفح ككلمات المرور، وسجل زياراتك، وغير ذلك من البيانات المؤقتة التي يحتفظ بها المتصفح. وفي حالة وجود أى بيانات أو ملفات ذات حساسية قم باستخدام البرامج التي تقوم بمحو الملفات والبيانات بشكل كامل بما لا يترك أثر يمكن أن يسّهل استرجاعها، لاحقا سنقوم بعرض البرمجيات التي تساعدك على هذا.

الاعتياد على استخدام البرمجيات الحرة

واحد من أهم التصرفات التي تساعدك على حماية بياناتك وخصوصيتك الرقمية هو استخدام البرمجيات الحرة. في حالة أنك تستخدم أحد توزيعات نظام تشغيل جنو/لنكس في الغالب سوف تعتمد بشكل كبير علي البرمجيات الحرة وخيارتك في أغلبها ستكون حرة، أما في حالة أنك تستخدم نظام تشغيل غير حر، كأنظمة تشغيل مايكروسوفت أو أبل، فستكون مضطر لأن تبحث عن بدائل أكثر أمانا للبرمجيات التي تستخدمها فوق هذه الأنظمة، كن حذرا جدا في استخدام برامج التواصل والدردشة والمتصفح وحاول أن تختار بدائل حرة تعمل مدعومة من نظام التشغيل الذي تستخدمه.

لا تجعل أجهزتك بين أياد متعددة

لا تجعل أجهزتك تتنقل بين أياد كثيرة، فبعض التصرفات البسيطة يمكنها أن تؤثر على أمان معلوماتك وبياناتك، لا تترك مثلا هاتفك المحمول دون كلمة مرور للدخول، ولا تتركه في مكان بعيد عن متناولك، وهو ما يجب أن تراعيه أيضا بالنسبة لجهاز الحاسوب المحمول الخاص بك، مع ضرورة أن تحتفظ ببطاقات الذاكرة والذاكرة الفلاشية في مكان آمن وبعيد عن أي يد عابثة.

ماذا بعد!..

في حالة أن تم العبث بأحد أجهزتك أو سرقته أو تعرضك لمساءلة قانونية، هناك بعض الاحتياطات التي تقلل من المخاطر التي قد تترتب على ذلك، ولاحقا سنتناول الجانب القانوني بالتفصيل، لكن على المستوى التقني وعادات الاستخدام، فإن هناك حاجة هامة لاستخدام كلمة سر قوية للولوج لأجهزتك المكتبية أو المحمولة، وحاول أن تستخدم أحد برمجيات محو الملفات والبيانات عن بعد كالتي تستخدم في الهواتف المحمولة، والتي توفر أيضا خاصية لتتبع الهاتف والإغلاق وغيرها من الإمكانيات.

كن حذرا!..

هناك مخاطر عديدة تحيط بأمنك الرقمي، ربما يكون مصدر هذه المخاطر أجهزة حكومية، أو أفراد عابثين من هواة انتهاك الخصوصية، أو ربما يكون مصدره شخص ما تحصل على بياناتك بطريق الصدفة نتيجة لعدم تأمينك لها، وفي جميع الحالات يجب أن تكون حذرا ومستعدا.

البرمجيات الخبيثة واحدة من أهم وأشهر المخاطر التي تؤثر على أمنك الرقمي، وهي برمجيات تتسلل إلى جهازك دون علمك وتتعدد أنواعها، وأهدافها؛ بعضها يكون بغرض تدميري، وتقوم بتدمير نظام التشغيل أو البرمجيات التي تستخدمها وأحيانا تحتاج لإعادة تهيئة القرص الصلب مما يجعلك تفقد بياناتك، وهناك برمجيات خبيثة تسعى لمراقبة تصرافتك كمستخدم ربما لمعرفة والمواقع التي تزورها، وهو ما يمكن استخدامه لاحقا ضدك، إذا ماتم

اتهامك بارتكاب بما يسمى (جرائم النشر الرقمي)، لمجرد معرفة تصرفاتك الشرائية على الشبكة، ويمكن أيضا أن يكون هدف هذا النوع من البرمجيات أن تعمل كـ "حصان طروادة" للتجسس عليك أثناء الاستخدام.

وهناك **برمجيات** تكون بها ثغرات أمنية والتي تكون عبارة عن مناطق ضعيفة بالبرمجية تمكن للمخترقين الولوج إلى حاسوبك أو الموقع الإليكتروني الخاص بك، وهذه العملية يمكن أن تتسبب في سرقة جميع الملفات المخزنة على حاسوبك أو الهاتف المحمول أو تدمير مدونتك أو موقعك، كما أنه يمكن أيضا الاعتماد على نوعية من البرمجيات الخبيثة التي تسمي "أحصنة طروادة" والتي تقوم بدورها بفتح ثغرة بالنظام تمكن المهاجم من النفاذ لبياناتك. وأيضا هناك "هجوم الرجل في الوسط" وهو مصطلح يطلق على نوع من أنواع التجسس، حيث يقوم المهاجم بالتسلل بين اثنين متحاورين في شبكة.

كيف يحدث اختراق/تجسس

هناك أكثر من طريقة للاختراق والتجسس، وأنواع مختلفة أيضا. وهنا سنتناول بعض الأنواع التي يتعرض لها الأفراد بشكل أساسي لتبسيط الطريقة، والتي ستساعدك لاحقا في ممارسات اعتيادية ستقلل من إمكانية تعرضك لخطر التجسس أو الاختراق.

الاختراق والتجسس

جميع الأجهزة تتصل عبر شبكات تمتلك معرف رقمي "IP Address" سواء كانت هذه الشبكة هي شبكة الإنترنت أو شبكة محلية أو أى من الشبكات الأخرى، وأيضا سواء كانت هذه الأجهزة التي نتحدث عنها هي حاسوب شخصي أو طابعة أو هاتف أو جهاز متصل بالشبكة، وهذا المعرف الرقمي يعتبر كعنوان للجهاز يتم التراسل بين الأجهزة المرتبطة بشبكة معينة بواسطة هذا المعرف الرقمي، يمكن أن تعتبر المعرف الرقمي أنه رقم لهاتفك الأرضي، لا يتكرر ويمكن الوصول إليك من خلاله.

في حالة أن هناك من يريد أن يقوم باختراق حاسوبك والتجسس عليك أو تدميره، سيقوم باستخدام المعرف الرقمي الخاص بك في ذلك، لأنه يمثل نقطة الوصول لحاسوبك، وهناك عدد من الطرق التي تمكن المخترقين من معرفة معرفك الرقمي، على سبيل المثال يمكن أن معرفته عن طريق بريد إليكتروني مرسل إليك، أو من خلال برامج التراسل غير الآمنة، أو بأي طريقة

أخرى فهناك الكثير من البرامج التي تقوم بهذه المهمة.

في حالة أن أحدهم حصل على معرفك الرقمي، تبدأ الخطوة الثانية وهي إيجاد منفذ (ثغرة) يدخل لك من خلالها، وهي في الغالب تكون ثغرة أمنية في نظام التشغيل أو في أحد البرمجيات المثبتة ومن خلالها يمكنه الدخول إلى حاسوبك.

بعض البرمجيات الخبيثة يمكنها أن تقوم بما ذكرناه سابقا، حيث يتم إرسال برمجية خبيثة إليك وزرعها بحاسوبك، ولهذه العملية طرق متعددة؛ على سبيل المثال عن طريق البريد الإليكتروني، أو تضمينها مع ملف أو برمجية معينة لاحقا، تقوم هذه البرمجية بفتح ثغرة في حاسوبك يتسلل منها المخترق، ومن خلالها يمكن أن يتم التجسس على كل ما تقوم به في حاسوبك ويمكن أن يتم نقل الملفات الموجودة به أو العبث بها وتغييرها أو أي من التصرفات التي يريدها المخترق.

لاحقا سنتناول طرق الحماية من هذه النوعية من الاختراقات والبرامج التي تساعد في هذا، لكن هناك بعض النصائح العامة مبدأيا ضعها في اعتبارك.

- **استخدم** دائما برامج مكافحة الفيروسات، والجدار الناري، وحدثها باستمرار.(1)
- **يفضل** الاعتماد على أنظمة تشغيل حرة، حيث أنها توفر قدر عالي من الأمان والحماية والثبات، يمكنك استخدام أحد توزيعات جنو/لينوكس.(2)
- **لا تقوم** بتثبيت أي برنامج إلا إذا كان موثوق به وحصلت عليه من موقع أو شخص موثوق به، حيث أنه يمكن أن يكون مضمن معه برمجية خبيثة كأحصنة طروادة.(3)
- **حاول** دائما أن تمتلك نسخة إحتياطية من ملفاتك الهامة، وقم بالاحتفاظ بها بعيدا خارج الحاسوب أو الهاتف المحمول الذي تستخدمه بانتظام، ويمكنك استخدام خدمات التخزين السحابية الحرة والموثوق بها كأوبنتو وان.(4)
- قم بتشفير الملفات والبيانات الحساسة والنسخ الاحتياطة، هناك عدد من البرمجيات الحرة التي توفر قدر عالي من الأمان يمكنك أن تستخدمها.(5)
- **ضع** كلمة سر قوية لإعدادات البيوس لحاسوبك، ولا تفعل الإقلاع من الأقراص المرنة وذاكرات اليو إس بي.
- **دائما** قم بوضع كلمة مرور للولوج لجهازك واجعلها صعبة ومكونة من حروف كبيرة و صغيرة ورموز وأرقام.(6)
- **لا تقم** بتحميل أى ملف أو برمجية وصلتك من خلال البريد الإليكتروني أو أحد الشبكات الاجتماعية إلا إذا كانت من مصدر موثوق به واستخدم برمجيات مكافحة الفيروسات أو الجدارات النارية.
- **احصل** على تحديثات البرامج التي تستخدمها بشكل مستمر، كثير من هذه التحديثات تكون بهدف سد ثغرات أمنية أو رفع مستوى الأمان بالبرمجية، خاصة وإن كانت التحديثات متعلقة بالمتصفحات وبرامج التواصل أو برمجيات مكافحة الفيروسات والجدارات النارية.
- **أثناء** اتصالاك بالإنترنت استخدم برمجيات للتعمية ينصح بحزمة TOR، حيث أنها توفر قدر عالي من التعمية أثناء استخدام الإنترنت.(7)
- **استخدام** برمجيات تراسل مؤمنة.(8)

التجسس على الهواتف المحمولة

الهواتف المحمولة أكثر قابلية للتجسس من أجهزة الحاسب الشخصي، وهذا يرجع لطريقة عملها وعمل نظم التشغيل المثبتة على هذه النوعية من الأجهزة. وبوجه عام يمكن لمقدم الخدمة أن يتتبعك وأن يتجسس على اتصالاتك بسهولة، وهناك بعض الحيل التي يمكن استخدامها للتحايل على هذا النوع من التجسس. لاحقا سنذكر روابط تشير إليها.

رقم IMEI هو رقم يميز كل الهواتف، وكل الهواتف لها رقم مميز، بطاقة SIM أيضا لها رقم مميز هذا، بالإضافة لرقم الهاتف، عبر هذه البيانات يمكن للحكومات/مزودي الخدمة أن يقوموا بالتتبع والتجسس على المستخدم، كما أن هناك الكثير من البرمجيات التي يمكن زرعها في هاتفك المحمول وتقوم بنقل مكالماتك ورسائلك والملفات والصور وأي من البيانات الموجودة على الهاتف.

في الهواتف الذكية يوجد عدد من الإمكانيات التي ربما تشكل تسهيل لعملية التجسس والتتبع؛ على سبيل المثال وجود خاصية تحديد المكان GPS. وفي حالة عدم وجود هذه الخاصية يكون تحديد المكان أقل دقة، خاصية Bluetooth يمكن أيضا أن يتم الدخول من خلالها والتجسس على المستخدمين، أيضا هناك العديد من التطبيقات التي تعمل على الهواتف الذكية ولا توفر حماية أو بها ثغرات يمكن من خلالها الحصول على كلمات السر الخاصة بالشبكات الاجتماعية أو البريد الإليكتروني على سبيل المثال.

هناك بعض البرمجيات والحيل التي تحاول تجاوز عائق التتبع والتجسس على الهواتف المحمولة، نذكر بعض من هذه النصائح العامة وسيتم وضع روابط للمزيد بهذا الصدد.

- **يجب** وضع كلمة سر قوية للهاتف، ويفضل استخدام نظام تشغيل مفتوح المصدر كأندرويد، حيث يتوافر به قدر لا بأس به من الحماية، ولا تنس أيضا أن تضع رقم التعريف الشخصي PIN.
- **تأكد** من جميع التطبيقات التي تعمل على هاتفك المحمول ولا تقوم بتنزيل أي برمجيات من مصادر غير موثوقة أو غير معروفة.
- **ينصح** باستخدام الهواتف التي تعمل بانظمة تشغيل مفتوحة ومتطورة، حيث أنها توفر خيارات وتطبيقات يمكنك استخدامها لحماية هاتفك مثل نظام تشغيل أندرويد.(9)
- **دائما** قم بتحديث جميع التطبيقات الموجودة بهاتفك ونظام التشغيل أيضا، حيث أن هذه التحديثات كثيرا ما تكون بهدف سد ثغرات أمنية أو تطوير الأمن والحماية للهاتف.
- **في حالة** إبحارك على الإنترنت من هاتفك المحمول، حاول أن تستخدم متصفح موثوق به وحر ويوفر قدر عال من الأمان، على سبيل المثال يمكنك استخدام متصفح فايرفوكس المخصص للهواتف الذكية.(10)
- **يفضل** عدم الاحتفاظ بأي بيانات أو معلومات أو صور حساسة على هاتفك وفي حالة وجودها يمكنك القيام بعمل تشفير لهذه الملفات وهناك بعض الأدوات المتاحة للقيام بهذه المهمه.(11)

- **لا تستخدم** برمجيات الترا سل غير الآمنة على هاتفك المحمول مثل whatsapp، وقم با ستخدام تطبيقات التوا صل المشفرة والتي توفر قدر أعلى من الأمان.(12)

- **ا ستخدام** برامج مكافحة الفيرو سات وبرامج تتبع الهاتف في حالة سرقته وإغلاقه، وبرمجيات المحو عن بعد، هذه الأ دوات مفيدة جدا في حالة سرقة هاتفك أو فقدة.(13)

- **قم** بتعطيل خا صية تحديد المكان GPS، حيث يمكن تتبعك من خلالها بسهولة، وأيضا عطل الشبكة اللا سلكية Wireless في حالة عدم ا ستخدامها ولا تقوم بالاتصال بشبكة wireless غير موثوق بها.

- **أثناء** ا ستخدام الإنترنت هناك تطبيق أيضا يمكن المستخدمين من ربط الهاتف المحمول بشبكة TORبسهولة.(14)

- **قدر** الإمكان حاول تخزين الملفات والبيانات الهامة على بطاقة SIM أو على بطاقة تخزين SD، حيث يمكنك مسح البيانات بشكل أ سهل.

- **ا ستخدم** بطاقات SIM غير مسجلة لحماية بياناتك الشخصية.

- **ا ستخدم** دائما بروتوكول HTTPS، حيث أنه يوفر قدر عال من الأمان في تصفح الإنترنت.

- **أغلق** خا صية تحديد المكان، ولا تقم بتفعيلها في أي تطبيق من التطبيقات المثبتة على الهاتف.

- **ا ستخدام** برمجيات تشفير الاتصالات والترا سل وتشفير الملفات.

- **يوجد** عدد من الأ دوات التي تقوم بمحو تفا صيل الصور وملفات الو سائط المتعددة، يمكنك ا ستخدام هذه الأ دوات عند الحاجة.

- **ا ستخدم** تطبيقات المحو والتتبع عن بعد والتي توفر لك خيارات مسح بيانات وملفاتك من الهاتف وتحديد مكانه في حالة سرقته أو فقده.

الشبكات الاجتماعية والتتبع والتجسس

تحتوي حسابات الشبكات الاجتماعية على الكثير من البيانات والتفاصيل والمعلومات التي يمكن تتبعك من خلالها، مهم جدا أن تكون حذرا في كل ما تضعه على حساباتك في الشبكات الاجتماعية، وبما أن موضوع الأمان الرقمي مترابط بشكل كبير فهناك عددا من النصائح العامة التي سنذكرها هنا؛ لكنها لا تؤخذ بمعزل عن النصائح السابقة، وهي خطوات مكملة لما سبق إلا أن البيانات المتعلقة بالشبكات الاجتماعية أكثر خطورة من تلك التي تقوم بحفظها على جهاز الحاسوب أو الهاتف أو أحد أدوات حفظ المعلمات الأخرى، نظر لما تتمتع به هذه الشبكات من خواص للنشر تسمح للآخرين بالإطلاع على بياناتك وما تنشره من محتويات وهو ما قد يضعك تحت طائلة القانون، خاصة إذا كنت تخضع لنظام قانوني يجرم نشر أنواع معينة من المحتويات.

- **أثناء** استخدامك للشبكات الاجتماعية، لا تترك أي معلومات في ملفاتك الشخصية يمكن الوصول من خلالها إليك، في حالة أن كنت تقوم بنشاط سياسي أو صحفي حاول أن تستخدم اسم مستعار ولا تترك بريدك الشخصي أو معلومة يمكن الوصل لك من خلالها.

- **قم** باختيار كلمات سر صعبة وقوية ويجب أن تحتوي على حروف كبيرة و صغيرة وأرقام ورموز. وقم بتغييرها كل فترة قصيرة.

- **قم** بتحديث التطبيقات الخاصة بالشبكات الاجتماعية دائما، فهذه التحديثات يمكن أن تكون لسد ثغرات أمنية أو تطويرات ترفع قدرة الحماية والأمان للتطبيق، وفي حالة أن كنت تستخدم هذه الشبكات من خلال المتصفح، دائما استخدم التصفح الآمن HTTPS واستخدم متصفح آمن ومفتوح المصدر كفايرفوكس.

- **اطلع** جيدا على خيارات الخصوصية التي توفرها الشبكات الاجتماعية ولا تتجاهلها، وحاول قدر الإمكان أن تحافظ على خصوصيتك ولا تجعل بياناتك متاحة للجميع.

- **بعض** الشبكات الاجتماعية تربط النشاطات التي تقوم بها مع موقعك، دائما قم بتعطيل هذا الخيار.

- **لا تترك** أي رسائل أو صور أو أي ملفات يمكنها أن تشكل خطورة عليك وقم بمحوها فورا.

- **كن** حذرا في تنزيل أو تثبيت أى برمجية تصلك عبر الرسائل في الشبكات الاجتماعية، والروابط غير الموثوق بها أيضا لا تقم بفتحها.

- **احذر** من الصفحات الوهمية التي ترسل إليك وتطلب إدخال كلمة السر، ولا تستخدم كلمات سرك إلا في المواقع الموثوق بها فقط.

- **هناك** تطبيقات ومواقع تطلب منك ربط حساباتك بالشبكات الاجتماعية بها، لا تقم بهذا إلا في حالة وجود ثقة كاملة بهذه النوعية من التطبيقات، واضطلع جيدا على التصاريح المتاحة لهذه التطبيقات.

نصائح قانونية حول الأمن الرقمي

ما سبق تقديمه من نصائح تقنية هدفه الأساسي تفادي الوقوع فريسة لانتهاك الحق في الخصوصية الرقمية، وكذلك حمايتك من الوقوع تحت طائلة القانون، خاصة إذا كنت تعيش في بلد مثل مصر، تفرض قيود عديدة على حرية النشر وحرية التعبير وحرية تداول المعلومات عبر الوسائل التقنية المتنوعة، وبالتالي يجب أن تكون مدركا لحقوقك القانونية إذا ما تعرضت للمساءلة بسبب محتوى قمت بنشره رقميا، أو إذا قام أحد الأشخاص أو الجهات باتهامك بارتكاب أحد جرائم النشر عبر وسيط رقمي عن طريق اختراق أحد حساباتك، أو التجسس على بياناتك واستخدامها في اتهامك، أو إذا قام أحدهم بتقديم بياناتك إلى أحد جهات التحقيق كدليل إدانة ضدك.

بماذا يمكن اتهامك؟..

تتنوع جرائم النشر الرقمي في قانون العقوبات المصري الذي يقيد حرية التعبير تحت دعاوى عديدة مثل حماية النظام العام، والسلم العام والآداب العامة، وغيرها من العبارات التي دائما ما تستخدم لفرض قيود على حرية الكلام، ومن أهم الأفعال التي يؤثمها قانون العقوبات -إذا ما تم اتيانها بإحدى طرق النشر، والتي من بينها بالطبع وسائل النشر الرقمي- التحريض بأنواعه المختلفة، والسب والقذف سواء للأفراد أو للجهات، وازدراء الأديان، ونشر الأخبار الكاذبة، وخدش الحياء، وانتهاك حرمة الآداب العامة، والإساءة لسمعة البلاد، والعيب في حق ملك أو رئيس دولة أجنبية، وإهانة رئيس الجمهورية، والعيب في حق ممثل لدولة أجنبية معتمد في مصر، وإهانة إحدى الهيئات النظامية، وإهانة موظف عام، والإخلال بمقام قاض، والتأثير في القضاة ورجال النيابة العامة والشهود والرأي العام، وخرق حظر النشر في جلسات المحاكم وتحقيقات النيابة، وجلسات البرلمان.

العلانية.. ركن أساسي في جرائم النشر الرقمي

لا تقوم جريمة النشر الرقمي إلا إذا توافر ركن العلانية، ويعني هذا أن يستطيع عدد من الأفراد تصفح ما قمت بنشره دون تمييز. وبالتالي يتوجب عليك قبل نشر أي محتوى على أحد الشبكات الاجتماعية مثل (فيسبوك) أن تكون متأكدا من الإعدادات التي من خلالها تحدد من يمكنه تصفح ما قمت بنشره. هل هم جميع مستخدمي الشبكة التي تستخدمها، أم أصدقاؤك فقط، أم أن لا أحد غيرك يمكنه مطالعة المحتوى الذي قمت بنشره. فإذا كان ما قمت بنشره يدخل في نطاق ما يعتبر من جرائم النشر، فإن جهة التحقيق وجهة المحاكمة يتوجب عليهما التأكد من إعدادات النشر قبل اتهام المستخدم المتهم أو إدانته بنشر محتوى مؤثم جنائيا. وتنظم المادة 171 من قانون العقوبات طرق العلانية على سبيل المثال وليس الحصر، حيث اعتبرت أن القول أو الصياح علنيا إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريق اللاسلكي أو بأية طريقة أخرى، ويكون الفعل أو الإيماء علنيا إذا وقع في محفل عام أو طريق عام أو في أي مكان آخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان، وتعتبر الكتابة والرسوم والصور، والصور الشمسية والرموز وغيرها من طرق التمثيل علنية إذا وزعت بغير تمييز على عدد من الناس، أو إذا عرضت بحيث يستطيع أن يراها من يكون في الطريق العام أو أي مكان مطروق أو إذا بيعت أو عرضت للبيع في أي مكان.

على سبيل المثال إذا تم اتهامك بنشر محتوى إليكتروني يقع تحت إحدى جرائم النشر السابق الإشارة إليها، وكان هذا النشر على موقع "فيسبوك"، لكنك قمت بتغيير الإعدادات بحيث لا يستطيع غيرك تصفح هذا المحتوى، أو سمحت لعدد محدود من أصدقائك فقط بالتصفح دون باقي مستخدمي الشبكة، فإن ذلك لا يدخل في نطاق طرق العلانية التي يشترط القانون توافرها لقيام الجريمة.

هل هناك فرق بين ما تحفظه على قرص صلب وما تنشره على أحد المواقع؟

بالطبع هناك فرق كبير، فأيا كان ما تقوم بحفظه على قرص صلب أو أسطوانة مدمجة أو جهاز الحاسوب أو الهاتف المحمول الخاص بك أو أي وسيلة من وسائل حفظ المعلومات الرقمية، فهو لا يعتبر نشرا ولا علانية، سواء كانت هذه المعلومات صورا أو مقاطع صوتية أو مصورة أو غيرها، وحتى وإن اعتبرت ضمن المحتويات التي يعتبر نشرها ارتكابا لإحدى جرائم النشر السابق الإشارة إليها.

فالحفظ في حد ذاته لا يثبت ركن العلانية بوصفه ركن جوهري في جريمة النشر، لأنه لا يثبت إتاحة هذا المحتوى للغير دون تمييز..

لكن احذر!

قد يكون المحتوى الذي تقوم بحفظه على أحد وسائل حفظ المعلومات والبيانات الرقمية هو صور لحساباتك على الشبكات الاجتماعية مثل (فيسبوك، تويتر ..إلخ) وقد تثبت هذه الصور قيامك بنشر محتوى مؤثم قانونا في تاريخ معين وهو ما قد تؤاخذ عليه إذا ما تم ضبطه بواسطة إحدى جهات الضبط.

أما ما تقوم بنشره على أحد مواقع الإنترنت، أو الشبكات الاجتماعية، بحيث أصبح متاحا للغير تصفحه دون تمييز، فهو يحقق ركن العلانية اللازم لقيام جريمة النشر.

هل تعتبر الرسائل ضمن طرق العلانية؟

تستطيع أن تقوم بإرسال محتوى رقمي إلى صديق/ة أو إلى عدد من الإصدقاء، سواء بواسطة البريد الإليكتروني، أو بواسطة خاصية الرسائل التي تتمتع بها بعض الشبكات الاجتماعية مثل فيسبوك وتويتر، ويتسائل البعض هل إذا كان المحتوى الذي قمت بإرساله مؤثم نشره قانونا، فعل تعتبر الرسائل مثل النشر المفتوح الذي يتيح لعدد من الناس تصفح ما قمت بنشره دون تمييز؟؟.

الأمر يتوقف على عدد من قمت بمراسلتهم وعلى طبيعة المحتوى الذي قمت بإرساله. فإذا كان

عدد من تلقى رسالتك محدود بمعنى فرد أو اثنان أو ثلاثة أفراد، فلا يعتبر الإرسال هنا علانية، أما إذا كان عدد من تلقوا رسالتك غير محدود ودون تمييز، كأن تقوم بإرسال رسالة بريد إليكتروني لكافة العناوين البريدية التي تحفظها بريدك، أو أن تقوم بإرسال رسالة لجميع أصدقائك على "فيسبوك" فهذا يعتبر نشرا بإحدى طرق العلانية، لانتفاء ركن الخصوصية.

أما من حيث طبيعة المحتوى الذي قمت بإرساله، فمثلا إذا قمت بإرسال صورة، أو مقطع صوتي، أو مقطع مصور أو غيرها، فهذا لا يثبت النشر بإحدى طرق العلانية، أما إذا كان ما قمت بإرساله هو رابط لموقع على شبكة الإنترنت أو صفحة على "فيسبوك"، أو حساب على موقع تويتر، أو قناة على موقع يوتيوب أو غيرها من المواقع والشبكات التي تتيح لعدد غير محدد من الناس تصفح محتواها، فإذا كان محتوى الرابط مؤثم قانونا فتقع جريمة النشر بإحدى طرق العلانية.

هل أنت مسئول عن التعليقات التي يكتبها أصدقاؤك على ما قمت بنشره؟؟

بالطبع أنت غير مسئول عن أي تعليق يكتبه أو ينشره أحد أصدقائك على ما قمت أنت بنشره، خاصة إذا كان محتوى التعليق مؤثم قانونا، فالجريمة شخصية، والعقوبة كذلك، ولا يؤاخذ أي شخص بما أتاه غيره من أفعال، وبالتالي تنحصر مسئوليتك القانونية فيما قمت أنت بنشره، وتنحصر مسئولية المعلق على ما قام بكتابته أو نشره في محتوى تعليقه.

إثبات جريمة النشر الرقمي

تعتبر جرائم النشر الرقمي من أكثر الجرائم صعوبة في الإثبات، وذلك لصعوبة السيطرة المادية على كل جوانبها، حيث يسهل سرقة بيانات أحد الأشخاص وعمل حساب على أحد الشبكات الاجتماعية بواسطتها، واستخدام هذا الحساب في نشر محتوى مؤثم قانونا، كما يسهل اختراق أحد هذه الحسابات واستخدامه في ذات الغرض، وهو ما قد يعرض صاحبه للمسائلة القانونية، لذا فإن تحقيق جرائم النشر الرقمي يحتاج إلى درجة عالية من الدقة والاستعانة بالخبرة الفنية لإثبات الجريمة ضد من يتهم بارتكابها، وذلك لأن الإدانة في الجرائم الجنائية يجب أن تبنى على الجزم واليقين، وإذا كان هناك شك في ارتكاب الشخص المنسوب إليه الاتهام بجريمة نشر رقمي فإن الشك يفسر لمصلحته.



القبض على المتهم بجريمة نشر رقمي

هناك ثلاث حالات للقبض على المتهم بارتكاب أي جريمة

الحالة الأولى.. هي ضبط المتهم متلبسا بارتكاب إحدى جرائم النشر الرقمي، وهي حالة غاية في الصعوبة على عكس الجرائم الاخرى، فمثلا يسهل ضبط متهم متلبسا بارتكاب جريمة سرقة، لو ضرب أو غيرها، أما جرائم النشر الرقمي فإنها من الجرائم المستمرة، وتقع الجريمة بفعل النشر، إلا أنه قد يتم اكتشافها من قبل السلطات المختصة بعد ذلك فترة زمنية، وبالتالي هناك صعوبة في تطبيق حالات التلبس عليها التي لا تنطبق إلا في ذات وقت ارتكاب الجريمة أو بعد وقوعها مباشرة وبفترة وجيزة جدا.

الحالة الثانية.. وهي استصدار إذن من النيابة العامة بالقبض على متهم بارتكاب جريمة نشر رقمي، وتنطبق هذه الحالة إذا انتفى التلبس بارتكاب الجريمة، فلا يجوز لرجال الضبط القبض على المتهم دون إذن من النيابة العامة.

الحالة الثالثة.. تكليف المتهم بالحضور أمام النيابة العامة لاستجوابه ثم الأمر بالقبض عليه أو إطلاق سراحه.

وبالتالي إذا خرج القبض على المتهم عن إحدى الحالات الثلاث سالفة البيان فإنه يكون باطل قانونا، ويحدث هذا إذا تم القبض عليه دون توافر حالة من حلات التلبس، أو قبل صدور إذن من النيابة العامة بالقبض عليه، وتبطل كافة الإجراءات المترتبة على هذا القبض الباطل، أو الأدلة المستمدة منه، فمثلا إذا تم القبض على متهم بارتكاب جريمة نشر رقمي بغير الطرق سالفة البيان، وتم التحفظ على هاتفه المحمول المسجل عليه حساباته على بعض شبكات التواصل الاجتماعي أو بريده الإلكتروني، وتم إثبات نشره محتوى مؤثم قانونا عبر استخدامه لإحدى حساباته عبر الهاتف المحمول، فإنه لا يمكن إدانته بنشر محتوى رقمي مؤثم قانونا نظرا

لأن إجراء التحفظ على الهاتف الذي يثبت ارتكاب الجريمة باطل، لأن عملية القبض عليه تمت بشكل باطل قانونا أيضا، والقاعدة أن كل ما ترتب على باطل فهو باطل.

تفتيش شخص ومسكن المتهم بارتكاب جريمة نشر رقمي

لا يجوز لرجال الضبط تفتيشك أو تفتيش مسكنك دون إذن من النيابة العامة، إلا إذا تم القبض عليك متلبسا بارتكاب الجريمة، وفي غير هذه الحالة يجب أن يصدر إذن بالتفتيش من النيابة العامة، ويجب أن يحدد الإذن النطاق الزمني لتنفيذه، بمعنى أن يتم التفتيش خلا 24 ساعة من صدور الإذن أو 48 ساعة وهكذا، وبالتالي إذا ذهب الماذون له بتفتيش مسكنك في تاريخ غير المحدد في إذن النايبة فإن التفتيش يقع باطلا.
كذلك فإن الإذن بالتفتيش بالنسبة لجرائم النشر الرقمي، يجب أن يشمل الأشياء التي يجب على الأذون له ضبطها، وغالبا ما تكون هذه الأشياء هي الحواسب، والهواتف المحمولة، والأسطوانات المدمجة، وبطاقات الذاكرة الرقمية، وغيرها من أدوات حفظ ونشر المعلومات والبيانات الرقمية.

ويجب على المأذون له بتفتيش مسكنك أن يدخل إلى المسكن برضائك أو برضاء أي شخص آخر من أسرتك تكون له صفتي الإقامة في المنزل وحيازته، فإذا لم يراع المأذون له بالتفتيش هذه القواعد السابقة جميعها، وقع التفتيش باطلا، وتبطل كافة الأدلة المستمدة منه.

استجواب المتهم في جرائم النشر الرقمي

تقوم النيابة العامة بالاستجواب، وهو أحد إجراءات التحقيق، ويكون عبارة عن مجموعة من الإسئلة يوجهها إليك المحقق لتجيب عليها، لكن احذر! فكل ما تقوله بمحض إرادتك في إجاباتك سوف تؤاخذ عليه إذا كان من شأنه الاعتراف أو الإقرار بارتكاب جريمة نشر رقمي، أو كان من شأنه أن يقود المحقق إلى دليل جديد ضدك.

كلمات المرور واسم المستخدم

ليس للمحقق أثناء استجوابك إجبارك على أن تقول أي شيء لا تريد أن تقوله، ويتضمن ذلك عدم أحقيته في إجبارك على إعطائه كلمات المرور وأسماء المستخدم بالنسبة لحساباتك على الشبكات الاجتماعية، أو بياناتك المحمية بكلمات مرور أخرى، وإذا تحصل المحقق على أيا منها أثناء استجوابك بإكراهك على ذلك، يبطل تحقيق النيابة، وتبطل كافة الإجراءات المترتبة عليه، وكذلك الأدلة المستمدة منه، لكن إذا أعطيته أيا منها بمحض إرادتك، فإن ما يترتب عليها من أدلة ضدك تكون صحيحة ويمكن للمحكمة أن تأخذ بها إذا قررت إدانتك.

ماذا يمكن أن يقود المحقق إلى أدلة جديدة ضدك؟؟

الاعتراف

قد يكون الدليل المقدم ضدك لجهة التحقيق عبارة عن أسطوانة مدمجة، وقد تكون الأسطوانة تحتوي على محتوى مؤثم نشره قانونا، إلا أن ذلك لا يكفي لإدانتك، لإن الأسطوانة في حد ذاتها لا تثبت قيامك بالنشر الذي يحقق ركن العلانية، لكنك إذا قامت بالاعتراف للمحقق بالنشر وكان الاعتراف صادرا عن أرادتك الحرة ودون إكراهك عليه، فإن ذلك يعتبر دليل كاف على النشر.

الإقرار

والإقرار قد يدعم أحد أدلة الإدانة الموجهة ضدك، كما قد يقود المحقق لدليل جديد، فعلى سبيل المثال إذا أقريت أمام المحقق بأنك تحتفظ ببعض البيانات أو المعلومات ذات الصلة بموضوع التحقيق، أو تحتفظ بكلمات مرور واسم المستخدم في منزلك، فإن ذلك قد يقود المحقق إلى قرار بتفتيش منزلك، أو اذا أقريت بأنك تملك بعض الحسابات على شبكات التواصل الاجتماعي، أو تملك موقع على الإنترنت مثلا، أو أنك قائم على إدارة إحدى صفحات "فيسبوك" فإن ذلك أيضا قد يقوده إلى قرار بإجراء التحريات الفنية حول المعلومات التي أدليت بها، أو بانتداب خبير فني لفحص هذه المواقع والحسابات وتفريغ محتواها.

هل يجوز إجراء التحريات حول نشاطك الرقمي؟

نعم يجوز لرجال الضبط القضائي إجراء التحريات حول جرائم النشر الرقمي، دون إذن من النيابة العامة، إلا أن ذلك مشروط بعدم انتهاك خصوصيتك أو التجسس عليك، وبالتالي تكون التحريات صحيحة من الناحية الإجرائية إذا وقعت على معلومات غير محمية بكلمات مرور أو غيرها من أدوات الحماية، أما الوصول إلى معلومات محمية من جانبك ولا يستطيع غيرك تصفحها، فهذا يتطلب إذن من النيابة العامة، وإلا وقع إجراء التحريات باطلا ولا يجوز أن يستمد منه دليل إدانة ضدك، وغالبا ما تقع التحريات الفنية على أرقام الهواتف التي من خلالها قمت بإنشاء حساباتك على الشبكات الاجتماعية، وبريدك الإليكتروني وغيرها، وكذلك المحتويات التي تم نشرها بواسطة هذه الوسائل.

هل جهات التحقيق مؤهلة فنيا للتحقيق في جرائم النشر الرقمي؟

بالطبع لا، فالمحقق لا يعرف كل شيء، خاصة إذا ارتبط التحقيق بمسألة فنية تحتاج إلى متخصص ليقول رأيه، وذلك في مسائل معينة، على سبيل المثال إذا أراد المحقق معرفة القائمين على إدارة صفحة معينة على موقع فيسبوك (أدمنز)، فهذا أمر لا يستطيع الوصول إليه إلا شخص متخصص في هذه المسألة، أو إذا أراد التأكد من أن الصوت الذي سمعه في أحد المقاطع الصوتية أو المصورة هو صوتك الحقيقي أم صوت شخص آخر، فهذه أيضا مسألة تحتاج لخبير فني للقيام بها.

ما العمل إذا؟..

إذا صادف المحقق مسألة فنية تحتاج إلى متخصص ليقول رأيه فيها، وجب عليه انتداب خبير لذلك وذلك وفقا للمادة 85 من قانون الإجراءات الجنائية، ويجب على المحقق أن يحضر أثناء عمل الخبير لمتابعته، وللتأكد من عدم انحيازه ضدك، وأنه يفحص ما تم تكليفه بفحصه بشكل موضوعي، كما يجب على الخبير أن يحلف اليمين أمام المحقق على أن يبدي رأيه بالذمة وعليه أن يقدم تقريرا مكتوبا برأيه الفني ويترتب على عدم حلف اليمين بطلان الدليل الفني المستمد مما قاله هذا الخبير، إلا أنه يجوز الأخذ به على سبيل الاستدلال بشرط أن يكون المحقق قد حضر مع الخبير أثناء قيامه بعمله، وإلا أصبح غير جائز الاستدلال به.

ماذا يجب أن يتضمنه تقرير الخبير الفني؟

- يجب أن تكون جميع المعلومات التي يتضمنها صحيحة من الناحية الفنية والعلمية.
- في حالة أن التقرير انتهى إلى إدانتك بجريمة نشر رقمي، يجب أن يكون الرأي الفني الذي انتهى إليه متوافقا ومطابقا للأدلة الأخرى، فإذا تناقض مضمونه مع مضمون الأدلة الأخرى لا يمكن الأخذ به كدليل إدانة.

(على سبيل المثال إذا أقريت أمام المحقق بأنك قمت بنشر محتوى مؤثم قانونا تحت عنوان معين وبمضمون معين وجاء تقرير الخبير النفي ليقول بلأن المحتوى منشور تحت عنوان آخر وبمضمون مختلف أو إذا تناقضت نتائج التقرير مع شهادة الشهود فإنه لا يجوز للمحكمة الحكم بإدانتك وإلا وقع حكمها باطلا)

- يجب أن يتضمن التقرير الفني جميع الألفاظ والعبارات والصور التي يتضمنها المحتوى الذي تم اتهامك بنشره.

هل لك الحق كمتهم في الاستعانة بخبير؟

نعم يعطيك قانون الإجراءات الجنائية الحق في أن تستعين بخبير استشاري، ولهذا الخبير الإطلاع على كافة أوراق القضية خاصة ما تم تقديمه للخبير الذي انتدبه المحقق؟.

ماذا إذا شعرت بأن الخبير المنتدب من جهة التحقيق منحاز ضدك؟

إذا شعرت بأن الخبير الذي انتدبته النيابة أو قاضي التحقيق غير موضوعي وغير أمين في عمله، وأنه يريد إدانتك لأي سبب، يمكنك أن تطلب من جهة التحقيق رد هذا الخبير، ويجب أن يكون لطلب الرد أسباب قوية، وعلى جهة التحقيق الفصل في هذا الطلب خلال ثلاثة أيام من تاريخ تقديمه.

قائمة لشرح أهم البرمجيات التي يمكنك استخدامها لأمنك الرقمي ومرتبطة بما تم ذكرة سابقا من نصائح

1- حماية الحاسوب من البرمجيات الخبيثة ومن المخترقين - عدة الأمان
https://securityinabox.org/ar/chapter_01

2- البرمجيات الحرة - عدة الأمان https://securityinabox.org/ar/chapter_01_4

3- الفيروسات والديدان وأحصنة طروادة - عدة الامان https://securityinabox.org/ar/chapter_01_1

4- تَدارُكُ فُقْدِ البيانات -عدة الأمان https://securityinabox.org/ar/chapter_05

5- تروكريبت - تخزين آمن للملفات https://securityinabox.org/ar/truecrypt

6- وضع كلمات سر قوية وحفظها https://securityinabox.org/ar/chapter_03

7- تور - شبكة المجهولية و تجاوز الرقابة https://securityinabox.org/ar/tor

8- بدْجن مع OTR - تراسل لحظي آمن https://securityinabox.org/ar/pidgin

9- الأجهزة التي تعمل بنظام تشغيل أندرويد http://www.android.com/devices/

10- متصفح فايرفوكس - نسخة تعمل على الهاتف المحمول http://www.mozilla.org/en-US/mobile/

11- تخزين المعلومات على هاتفكم الذكي https://securityinabox.org/ar/node/2945

12- التواصل (بالصوت والرسائل) عبر الهواتف الذكية https://securityinabox.org/ar/chapter_11_02

13- تطبيق avast للحماية من البرمجيات الخبيثة ووالحماية من السرقة
http://www.avast.com/free-mobile-security

14- برنامج Avira للحماية من السرقة
http://www.avira.com/en/download/product/avira-free-android-security/

14- تصفّح الإنترنت بأمان عند استخدام الهواتف الذكية
https://securityinabox.org/ar/node/2948

للمزيد:

1 - عدة الأمان - أدوات وممارسات للأمن الرقمي https://securityinabox.org/ar

2 - دليل عملي لحماية هويتك والحفاظ على سريتك أثناء تواجدك على الإنترنت وأثناء استخدامك للتليفون المحمول
https://www.accessnow.org/pages/protecting-your-security-online

عن برنامج الحريات الرقمية

يعمل برنامج الحريات الرقمية بمؤسسة حرية الفكر والتعبير، على الدفاع عن حق الأفراد في الوصول إلى واستخدام وإنشاء ونشر محتوى رقمي، واستخدام أي حواسيب أو أجهزة إليكترونية، أو برمجيات أو شبكات اتصالات سلكية ولاسلكية.

ويأتي اهتمام مؤسسة حرية الفكر والتعبير بالحريات الرقمية، من ارتباطها بكثير من الحقوق والحريات الأخرى التي تدخل في نطاق اهتمام المؤسسة، كالحق في المعرفة وحرية الإعلام، وحرية الرأي والتعبير، والحريات الأكاديمية.

الأهداف العامة للبرنامج

إتاحة المعلومات حول الحقوق الرقمية

يعمل البرنامج على إتاحة المعلومات حول مفاهيم الحريات الرقمية ومبادئها، من خلال إصدار مواد مطبوعة أو تنظيم لقاءات عامة.

حماية الحريات والدعم القانوني

العمل على حماية حريات مستخدمي وسائل الاتصالات، مثل الحق في التعبير والحق في الخصوصية وحماية البيانات، وحرية تداول المعلومات. والعمل على وقف كل أشكال الرقابة أو الملاحقة الأمنية أو القانونية لأي من مستخدمي الإنترنت أو أي وسيلة اتصالات أخرى.

نشر ثقافة المصادر الحرة

يعمل البرنامج على نشر ثقافة المصادر الحرة في إنتاج المحتوى الإلكتروني أو البرمجيات، ورفع الوعي وتشجيع الاعتماد على رخص المصادر المفتوحة في النشر الإلكتروني بمختلف أنواعه.

تمكين الأفراد

يسعى البرنامج لتمكين الأفراد من حقوقهم الرقمية عبر الضغط لتحسين الجوانب السياسية والتشريعية المنظمة لقطاع الاتصالات وتكنولوجيا المعلومات في مصر.

إتاحة استخدام الطيف الترددي (الموجات الراديوية)

العمل على إطلاق حرية استخدام الموجات الراديوية، خاصة فيما يتعلق بإنشاء "راديو الهواة" وما يرتبط بها من حرية التعبير وحرية الإعلام، ودعم الإعلام المجتمعي والمحلي